February 16, 2001

MEMORANDUM TO: William D. Travers
Executive Director for Operations

FROM: Stephen D. Dingbaum
Assistant Inspector General for Audits

SUBJECT: REVIEW OF NRC'S WEB SITE PRIVACY POLICY: INTERNET COOKIES (1-IA-08)

Attached is the Office of Inspector General's audit report titled, *Review of NRC's Web Site Privacy Policy: Internet Cookies.*

We conducted our review to comply with the requirements of the Treasury and General Government Appropriations Act, 2001 (HR 5658) passed as Public Law 106-554, on December 21, 2000. Section 646 required disclosing the collection by NRC and/or third parties, of personally identifiable information on individuals who visit the agency's web site.

Our review identified that neither NRC nor its third parties collect personally identifiable information on the agency's web site users. Information is collected for statistical purposes only to include the name of the domain; the type of browser and operating system used to access the site; and the date and time the user accesses the site. The report makes two recommendations.

If you have any questions, please call me at 415-5915.

Attachment: As stated

cc: R. McOsker, OCM/RAM
B. Torres, ACMUI
B. Garrick, ACNW
D. Powers, ACRS
J. Larkins, ACRS/ACNW
P. Bollwerk III, ASLBP
K. Cyr, OGC
J. Cordes, Acting OCAA
S. Reiter, Acting CIO
J. Funches, CFO
P. Rabideau, Deputy CFO
J. Dunn Lee, OIP
D. Rathbun, OCA
W. Beecher, OPA
A. Vietti-Cook, SECY
F. Miraglia, DEDR/OEDO
C. Paperiello, DEDMRS/OEDO
P. Norry, DEDM/OEDO
J. Craig, AO/OEDO
M. Springer, ADM
R. Borchardt, OE
G. Caputo, OI
P. Bird, HR
I. Little, SBCR
W. Kane, NMSS
S. Collins, NRR
A. Thadani, RES
P. Lohaus, OSP
F. Congel, IRO
H. Miller, RI
L. Reyes, RII
J. Dyer, RIII
E. Merschoff, RIV
OPA-RI
OPA-RII
OPA-RIII
OPA-RIV

February 16, 2001

MEMORANDUM TO: William D. Travers
Executive Director for Operations

FROM: Stephen D. Dingbaum
Assistant Inspector General for Audits

SUBJECT: MEMORANDUM REPORT: REVIEW OF NRC'S WEB SITE PRIVACY POLICY: INTERNET COOKIES (OIG-01-A-08)

This report provides the results of the Office of the Inspector General's (OIG) review of the Nuclear Regulatory Commission's (NRC) web site privacy policy. OIG found that NRC complies with Federal web site privacy policies. NRC has its privacy statement disclosed on its principal web site. Neither NRC nor its third parties collect personally identifiable information on individuals who visit its web site. Except for authorized investigations, and the gathering of site usage statistics, no other attempt is made to identify individual users or their usage habits. Information is collected for statistical purposes only and include: the name of the domain; the type of browser and operating system used to access the site; and the date and time the user accessed the site. However, NRC does not have a Management Directive covering this area. Therefore, the agency does not have policy guidance written in its directive system that establishes controls over or prohibits NRC and third parties from collecting personally identifiable information from visitors to the NRC web site. The report makes two recommendations.

PURPOSE

This review complies with the requirements of Public Law 106-554, *Treasury and General Government Appropriations Act, 2001 (HR 5658)*, passed on December 21, 2000. The Act requires the Inspector General of each department or agency to submit to Congress, within 60 days of its enactment, a report that discloses any activity of the applicable department or agency relating to: (1) the collection or review of singular data, or the aggregate lists that include personally identifiable information, about individuals who access any Internet site of the department or agency; and (2) agreements with third parties, including other government agencies, to collect, review, or obtain aggregate lists or singular data containing personally identifiable information relating to any individual's access or viewing habits for governmental and non-governmental Internet sites.

BACKGROUND

On June 2, 1999, the Office of Management and Budget (OMB) issued Memorandum M-99-18. This memorandum directed agencies to post:

- privacy policies to their agency's principal web site by September 1, 1999;
- privacy policies to any other known, major entry points to their web sites by December 1, 1999, as well as any web page where they collect substantial personal information from the public;
- policies that clearly and concisely inform visitors to the web sites what information the agency collects about individuals, why the agency collects it, and how the agency will use it; and
- policies that are clearly labeled and easily accessed when someone visits a web site.

Personal information is often collected at web sites in a file called a "cookie." A cookie is placed on a web user's hard drive by a web site to monitor access to the site, usually without the user's knowledge. Personal information can include an individual's name, e-mail address, postal address, telephone number, social security number, and a credit card number. Cookies are categorized into two main types: session and persistent. A session cookie is a file that tracks a user's activity during a visit to a web site but expires when the user leaves the web site. A persistent cookie lasts a fixed period of time, possibly for years and across different web sites. Potentially, many laws enacted to safeguard a citizen's right to privacy would be violated by establishing a persistent cookie.

On June 22, 2000, OMB issued Memorandum M-00-13, providing guidance relating to the collection of information by Federal web sites using cookies. This OMB guidance states that cookies should not be used at Federal web sites unless clear and conspicuous notice is given and the following conditions are met: (1) there is compelling need to gather the data on the site; (2) the agency takes appropriate and publicly disclosed privacy safeguards for handling information derived from cookies; and (3) the head of the agency has personally approved the use of cookies. In addition, the guidance requires that the agency incorporate privacy policy compliance information into its annual budget submission, beginning in Fall 2000.

RESULTS

Federal privacy policy disclosed on NRC's principal web site

NRC has a privacy policy statement posted on the home page of its web site that clearly advises visitors of the use of personally identifiable information. In both August 1999 and December 1999, the privacy policy was reviewed by the Office of the Chief Information Officer (OCIO) to ensure compliance with M-99-18.

OCIO reviewed the web pages where NRC requests personally identifiable information to ensure: (1) that the privacy policy is posted and that the guidance and model language was used on the policy; and (2) that the policy is linked to all pages that request personal

information. Information is collected for statistical purposes only to include: the name of the domain; the type of browser and operating system used to access the site; and the date and time the user accessed the site. Further, NRC complied with the June 2000 OMB request to include privacy policy compliance information in the agency's information technology budget submission for FY 2002.

Collection of personally identifiable information and agreements with third parties

OMB guidance prohibits the use of cookies at Federal web sites without adequate notice. OCIO assured OIG that neither NRC nor its third party contractors send cookies. OIG tested the web site for cookies both internally using NRC computers and externally from personal computers to verify that neither NRC nor its third party contractors send cookies. Our test procedures were consistent with those used by GAO to conduct similar tests. Our tests results found that, in compliance with OMB requirements, neither the NRC web site nor the third party contractors place cookies on users computers, nor does NRC collect personally identifiable information. In addition to testing for cookies, OIG requested and received confirmation from NRC that none of its contractors involved with the NRC web pages send cookies. Given that the National Laboratories are under the Department of Energy (DOE), we also confirmed that the DOE OIG included the Laboratories in its audit for collection of personally identifiable information. Except for the gathering of site usage statistics, no other attempt is made to identify individual users or their usage habits.

However, in reviewing the agency's Management Directives, OIG found that the agency does not have a directive to ensure the proper use of personally identifiable information. OIG was informed by OCIO that the privacy policy will be included as part of Management Directive 2.6 *NRC Information Resources Management Program,* which is currently being written. OIG was also informed that NRC contracts do not presently establish controls over, or prohibit the use of cookies because the legislation was only recently enacted. However, agency managers informed us that guidance covering the use of personally identifiable information will be issued in the near future.

CONCLUSION

NRC has a privacy statement that clearly informs users how NRC handles information during the user's visit to the web site. There are links to the major pages in the web site back to the privacy statement on the home page. Cookies are not sent to the user's computer to track any personally identifiable information. Only an operational log is used to generate site usage statistics.

However, NRC should institutionalize its privacy policies in the agency's directives system. In addition, even though we were assured at the entrance conference that all future contracts will include language prohibiting persistent cookies, this prohibition should also be a written policy in the agency's Management Directive system. These measures would increase public confidence that NRC protects the privacy of citizens when they visit its web site.

MANAGEMENT COMMENTS

At the exit meeting on February 12, 2001, management agreed with our recommendations and provided comments which have been incorporated in this report. Agency managers elected not to provide written comments to the draft report. They also informed OIG of their plans to issue interim guidance to cover this area until the Management Directive system is updated.

RECOMMENDATIONS

OIG recommends that the Executive Director for Operations:

(1) Include language in a Management Directive and in future NRC contracts to establish management controls over or prohibit NRC and third party contractors from collecting personally identifiable information from visitors to the NRC web site.

(2) Incorporate guidance into a Management Directive by September 1, 2001.

Please provide information on actions taken or planned on each of the recommendations directed to your office by March 16, 2001. Actions taken or planned are subject to OIG follow up.

SCOPE/ CONTRIBUTORS

This review focused on whether the NRC was following OMB's Memorandum 99-18 and Memorandum 00-13 addressing privacy policies on Federal web sites.

To complete our objectives we evaluated NRC's web site to determine if the privacy policy was: (1) clearly labeled; (2) easily accessed; (3) informed visitors about the information NRC collects; and 4) posted at major Web pages within the web site. We also reviewed OMB's guidance on privacy policies. We researched GAO reports and OIG reports concerning privacy and Internet cookies. We conducted interviews with staff as needed and reviewed all NRC pertinent documents concerning privacy and cookies. We tested to determine if NRC, its contractors, or the National Laboratories were using cookies to collect personally identifiable information.

We evaluated the management controls with regard to NRC's web site privacy policy and conducted our work from January 2001 to February 2001 in accordance with generally accepted Government auditing standards. This review was conducted by Corenthis Kelley, Team Leader, Beth Serepca, Audit Manager, and Vicki Foster, Management Analyst.

If you have any questions or concerns with regard to this report, please contact, Corenthis Kelley at 415-5977 or me at 415-5915.

Attachment
Recommendation Resolution Procedures

Instructions for Responding to OIG Report Recommendations

Instructions for Action Offices

Action offices should provide a written response on each recommendation within 30 days of the date of the transmittal memorandum or letter accompanying the report. The concurrence or clearance of appropriate offices should be shown on the response. After the initial response, responses to subsequent OIG correspondence should be sent on a schedule agreed to with OIG.

Please ensure the response includes:

1. The report number and title, followed by each recommendation. List the recommendations by number, repeating its text verbatim.

2. A management decision for each recommendation indicating agreement or disagreement with the recommended action.

a. For agreement, include corrective actions taken or planned, and actual or target dates for completion.

b. For disagreement, include reasons for disagreement, and any alternative proposals for corrective action.

c. If questioned or unsupported costs are identified, state the amount that is determined to be disallowed and the plan to collect the disallowed funds.

d. If funds put to better use are identified, then state the amount that can be put to better use (if these amounts differ from OIG's, state the reasons).

OIG Evaluation of Responses

If OIG concurs with a response to a recommendation, it will (1) note that a management decision has been made, (2) identify the recommendation as resolved, and (3) track the action office's implementation measures until final action is accomplished and the recommendation is closed.

If OIG does not concur with the action office's proposed corrective action, or if the action office fails to respond to a recommendation or rejects it, OIG will identify the recommendation as unresolved (no management decision). OIG will attempt to resolve the disagreement at the action office level. However, if OIG determines that an impasse has been reached, it will refer the matter for adjudication to the Chairman.

Semiannual Report to Congress

In accordance with the Inspector General Act of 1978, as amended, OIG is required to report to Congress semiannually on April 1 and October 1 of each year, a summary of each OIG report issued for which no management decision was made during the previous 6-month period. Heads of agencies are required to report to Congress on significant recommendations from previous OIG reports where final action has not been taken for more than one year from the date of management decision, together with an explanation of delays.

Document Location: G:\AUDIT\01-A-08\Final Memorandum Report.wpd

Distribution
AIGA Chron
OIG Chron
BSerepca
VFoster
CKelley

OIG	OIG	OIG	OIG	OIG	OIG	OIG
VFoster	BSerepca	CKelley	RIrish	SDingbaum	DLee	HBell
02/ /01	02/ /01	02/ /01	02/ /01	02/ /01	02/ /01	02/ /01

OFFICIAL FILE COPY